1:19MJ4233-JDG

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF OHIO EASTERN DIVISION

I, Bryon Green, hereafter "Affiant," being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a United States Postal Inspector and have been so employed since October 2006, presently assigned at Cleveland, Ohio to investigate Prohibited Mailing offenses. I have received training in the detection and investigation of prohibited mailing offenses. I have worked U.S. Postal Service related investigations for approximately 13 years, during which time I have been the case agent for investigations leading to prosecution in U. S. District Court, as well as state courts.

2. As a Postal Inspector, I have also conducted online investigations, analyzed pen register and telephone toll data, analyzed financial records, executed controlled deliveries of controlled substances, interviewed witnesses, drafted and executed search warrants, seized illegal drugs and other evidence of drug violations in physical and electronic sources, processed seized evidence, supervised the purchase of controlled substances by confidential sources, conducted undercover purchases of controlled substances in person and online, and debriefed persons arrested and convicted of drug trafficking offenses regarding their illegal activity.

3. Through investigation and training, I have become familiar with the types and amounts of profits made by drug traffickers and the methods, language, and terms that are used to disguise their illegal activity. I know that persons engaged in drug trafficking require expedient forms of communication to maintain an adequate and consistent supply of drugs from sources, and to effectively market those drugs to customers.

4. Your Affiant knows based on training and experiences those individuals who traffic in one controlled substances such as fentanyl often traffic and possesses other controlled substances and controlled substance analogues, particularly synthetic narcotics.

5. Furthermore, based on my training and experience that individuals who engage in unlawful activity on the internet (including the dark net) sometimes also use the expertise that they learn to engage in other criminal activity online.

6. This Affidavit is offered in support of a Criminal Complaint charging Defendant JERRY BRIAN STARR with Conspiracy to Possess with Intent to Distribute and to Distribute Controlled Substances, in violation of 21 U.S.C. § 846, and distribution of a controlled substance, in violation of 21 U.S.C. §§ 841(a)(1) and (b)(1)(C). As further detailed below, your Affiant submits that there is probable cause to believe that from on or about May 10, 2018 to March 6, 2019, Defendant did knowingly and intentionally combine, conspire, confederate, and agree with others to distribute and possess with the intent to distribute mixtures or substances containing controlled substances including:

- Fentanyl
- Black Tar Heroin
- Methamphetamine
- Oxycodone
- Ambien
- Dilaudid

All in violation of Title 21, United States Code, Sections 841(a)(1) and (b)(1)(C), and 846.

7. The facts set forth below are based upon your Affiant's personal knowledge learned through the course of the investigation as well as information obtained from law enforcement and additional sources.

8. This Affidavit is being submitted for the limited purpose of informing the court of the evidence establishing probable cause for a violation of federal criminal law. Since this affidavit is for

this limited purpose, your Affiant has not included each and every fact known concerning this investigation.

BACKGROUND CONCERNING DARK NET AND CRYPTOCURRENCY INVESTIGATIONS

9. The "clear" or "surface" web is part of the internet accessible to anyone with a standard browser and that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods.

10. The dark net is accessible only with specific software, configurations, and/or authorization, including non-standard communications protocols and ports, such as a TOR ("The Onion Router") browser. A TOR browser is designed specifically to facilitate anonymous communication over the internet. In order to access the TOR network, a user must install TOR software either by downloading an add-on to the user's web browser or by downloading the free "TOR browser bundle." Use of the TOR software bounces a user's communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user. Because of the way TOR routes communications through other computers, traditional IP identification techniques are not viable. When a user on the TOR network accesses a website, for example, the IP address of a TOR "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that TOR exit node IP address. A criminal suspect's use of TOR makes it extremely difficult for law enforcement agents to detect a host, administrator, or user actual IP address or physical location.

11. Dark net marketplaces operate on the dark net. These sites are generally only accessible through the input of specific addresses in a TOR browser. The dark net marketplaces function primarily as black markets, selling or brokering transactions involving drugs, cyber- arms,

weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the occasional sale of legal products. Dark net vendors (also known as distributors) operate on these dark net markets as sellers of these goods. They provide detailed information about their wares on these sites, including listings of their drugs for sale, (contact information such as TOR-based email or encrypted messaging applications), and the prices and quantities of drugs for sale in bitcoins. Customers purchase these goods using a computer or smartphone.

12. Your affiant is aware that some dark net marketplace vendors conduct the entirety of their transactions on the marketplace. Other vendors use the sites as an advertising base and messaging system and conduct their financial business in peer-to-peer transactions in order to avoid using third party escrow systems that they believe could be subject to law enforcement seizures as well as thefts, hacks, and scams.

13. Bitcoin (BTC)[1] is a type of virtual currency, circulated over the internet. Bitcoin is not issued by any government, bank, or company, but rather is controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

14. Bitcoin are sent to and received from BTC "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the Bitcoin address. Only the holder of an address' private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple BTC addresses at any given time and may use a unique Bitcoin address for each and every transaction.

---

[1] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

15. To acquire bitcoin, a typical user purchases them from a virtual[2] currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients' identities.

16. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender's private key, across the peer-to- peer BTC network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender's own private key. This information on its own rarely reflect any identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

17. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to third party companies that generally collect identifying information about their customers and are responsive to legal process.

---

[2] Bitcoins can accurately be referred to as a virtual, digital, and/or cryptographic currency.

18. Dark net marketplace buyers and sellers generally use bitcoin or some other form of cryptocurrency to conduct their transactions. Bitcoin is a decentralized digital/virtual currency that uses cryptography to secure the transactions and to control the creation of additional units of the currency. The digital currency gives the vendor and customer a perceived sense of anonymity. However, before a customer can make a purchase on a dark net marketplace, they must first convert fiat currency, such as United States Dollars, into the digital currency accepted on the market place. Dark net marketplace vendors also often have to convert the bitcoins that they earn through their sales into legal currency. These conversions generally take place on bitcoin exchangers, businesses who take bitcoin and give a certain amount of legal currency (such as the U.S. dollar) back at a set exchange rate and for a certain fee.

19. Your affiant is aware that individuals conducting business in this manner must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving bitcoin. Users of bitcoin must establish electronic wallets to receive and send the bitcoin during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, or computers. They may also be stored on third party wallet providers (such as Armory). Individuals often associate email accounts with these wallet providers and store information relating to that wallet on their email account. Your affiant is also aware that individuals conducting business by bitcoin can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. They are also often stored on email accounts, cloud or shared drives stored online (such as Google Drive), and other online storage mediums.

FACTS AND CIRCUMSTANCES ESTABLISHING PROBABLE CAUSE

20. The United States Postal Inspection Service (USPIS), the Department of Homeland

Security Investigations (HSI), Federal Bureau of Investigation (FBI), and Internal Revenue Service (IRS) are engaged in online undercover investigations targeting narcotics vendors on dark net marketplaces. These marketplaces are commonly used to facilitate purchases of narcotics and other illicit goods via vendors who operate 'stores' using monikers.

21. One such moniker on a known dark net marketplace is for the purposes of this affidavit referred to as "Moniker1." Moniker1 is a dark net market vendor that previously operated on the defunct "Dream" marketplace for approximately six years. "Dream" was a marketplace on the dark net that facilitated the sale of illegal narcotics until it shut down in April of 2019. According to Moniker1's vendor Dream Market profile, Moniker1 has previously operated stores on various other dark net markets such as the Black Market Reloaded and Agora Market that facilitated the sale of illegal narcotics. Moniker1 makes periodic updates to the Moniker1 vendor profile. This is used as a mass communication method to apprise customers of changes in order protocol, shipping issues, and all other business-related correspondence. Moniker1's Dream Market profile references another individual that assisted in the operation of the account indicating that more than one person is responsible for operating the store.

22. As of March 29, 2019, the Moniker1 profile indicated the store has conducted 900 verified transactions on the Dream Market, with 500 reviewed transactions.[3] His profile also shows records indicating a total of 1,400 sales of illegal narcotics across multiple dark net marketplaces, including for fentanyl, heroin, and methamphetamine. The only products listed for sale by Moniker1 are illegal narcotics. Moniker1 advertises the narcotics with photographs and detailed descriptions of each drug. Moniker1 advertises the following items for sale:

- Fentanyl
- Black Tar Heroin

[3] Similar to vendors on legitimate sites like Amazon and eBay, customers of a particular vendor can leave reviews for the transaction. Customers commonly review the speed of shipment and quality of illegal narcotics received from the seller. In Your Affiant's experience, the number of reviews for a vendor is generally lower than the total number of transactions, as leaving a review is voluntary.

- Methamphetamine
- Oxycodone
- Ambien
- Dilaudid

23. On May 10, 2018, your Affiant and Homeland Security Investigations Special Agent M. Grote (SA Grote) conducted an undercover purchase of 2 grams of black tar heroin from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District of Ohio.

24. On May 16, 2018, your Affiant recovered U.S. Postal Service Priority Mail parcel destined for the undercover address in the Northern District of Ohio resulting in the recovery of 1.99 grams of a mixture or substance containing heroin. The subject parcel is further described as a small U.S. Priority Mail parcel bearing the return address in California.

25. On July 9, 2018, your Affiant and SA Grote conducted an undercover purchase of 14 grams of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District of Ohio.

26. On Jul 19, 2018, your Affiant recovered U.S. Postal Service Priority Mail destined for the undercover address in the Northern District of Ohio resulting in the recovery of 14.16 grams of 98% pure methamphetamine hydrochloride. Forensic laboratory services identified latent prints on the exterior of the parcel belonging to JERRY BRIAN STARR.

27. On July 22, 2018, your Affiant conducted an undercover purchase of 20 grams of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District ofOhio.

28. On Jul 27, 2018, your Affiant recovered a first class stamped U.S. Postal Service Priority Mail parcel in the Northern District of Ohio resulting in the recovery of 21.44 grams of methamphetamine. The subject parcel is further described as a small U.S. Priority Mail parcel

bearing the return address in California. The parcel listed no tracking number, however the postage was paid at a kiosk inside the Post Office. Video Surveillance identified an individual, later identified as JERRY BRIAN STAR, using a prepaid credit card to pay for postage. Forensic laboratory services identified latent prints belonging to JERRY BRIAN STARR on the exterior of parcel and the interior packaging used to conceal the methamphetamine.

29. On August 15, 2018, your Affiant conducted an undercover purchase of 4.25 ounces of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District ofOhio.

30. On August 20, 2018, your Affiant recovered U.S. Postal Service Priority Mail parcel destined for the undercover address in the Northern District of Ohio. The parcel contained 112.54 grams of methamphetamine. The subject parcel is further described as a small U.S. Priority Mail parcel bearing the return address in California.

31. On October 14, 2018, Denver Postal Inspectors conducted an undercover purchase of .8 grams of methamphetamine from Dream Market vendor Moniker1. Denver Postal Inspectors subsequently received a U.S. Postal Service Priority Mail containing .8 grams of methamphetamine. Video Surveillance identified an individual, later identified as JERRY BRIAN STARR, using a credit card to pay for postage inside the Post Office on October 14, 2018.

32. On January 14, 2019, your Affiant conducted an undercover purchase of 2.5 grams of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District ofOhio.

33. On January 18, 2019, your Affiant recovered a U.S. Postal Service Priority Mail parcel destined for the undercover address in the Northern District of Ohio resulting in the recovery of 2.5 grams of methamphetamine. This parcel was sent from a California Post Office. Video Surveillance identified an individual, later identified as JERRY BRIAN STARR, using a credit card to pay for postage. Forensic laboratory services identified latent prints belonging to JERRY BRIAN STARR

on the interior packaging used to conceal the methamphetamine.

34. On February 14, 2019, your Affiant conducted an undercover purchase of 2.5 grams of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District ofOhio.

35. On February 18, 2019, your Affiant recovered U.S. Postal Service Priority Mail parcel destined for the undercover address in the Northern District of Ohio resulting in the recovery of 2.5 grams of methamphetamine. This parcel was sent from a California Post Office. Video Surveillance identified an individual, later identified as JERRY BRIAN STARR, using a credit card to pay for postage.

36. On March 3, 2019, your Affiant conducted an undercover purchase of 8 grams of methamphetamine from Dream Market vendor Moniker1. Your Affiant requested the purchase be sent to an undercover address located in the Northern District ofOhio.

37. On March 6, 2019, your Affiant recovered a U.S. Postal Service Priority Mail parcel destined for the undercover address in the Northern District of Ohio resulting in the recovery of 8 grams of methamphetamine. This parcel was sent from a California Post Office. Video Surveillance identified an individual, later identified as JERRY BRIAN STARR, using a credit card to pay for postage. Forensic laboratory services identified latent prints belonging to JERRY BRIAN STARR on the interior packaging used to conceal the methamphetamine.

38. Your Affiant used JERRY BRIAN STARR's California Driver's License photo, along with photos from JERRY BRIAN STARR's Facebook account, when reviewing surveillance video of the narcotics mailings described above to associate JERRY BRIAN STARR as the mailer. Your affiant believes based on the surveillance video captured of JERRY BRIAN STARR and the fingerprints identified on the exterior and interior of the parcels described above, JERRY BRIAN STARR is responsible for the trafficking of narcotics from California into the Northern District of Ohio.

39. For the foregoing reasons, Affiant respectfully submits that there is probable cause that JERRY BRIAN STARR committed the following federal offenses: Conspiracy to Possess with Intent to Distribute and to Distribute Controlled Substances, in violation of 21 U.S.C. § 846; Distribution of a Controlled Substance, in violation of 21 U.S.C. §§ 841(a)(1) & (b)(1)(C).

BRYON GREEN
POSTAL INSPECTOR

On October 04th, 2019, this affidavit was sworn to by the affiant, who did no more than attest to its contents pursuant to Crim. R. 4.1 (b)(2)(A), by telephone after a document was transmitted by email, per Crim R. 4.1

JONATHAN D. GREENBERG
U. S. MAGISTRATE JUDGE